Comments Received on SP 800-130

A Framework for Designing Cryptographic Key Management Systems

On 7/12/10 5:08 PM, "Bob.Nixon@Emulex.Com" <Bob.Nixon@Emulex.Com> wrote:

Following are a number of comments on Draft SP 800-130 (June 16, 2010). Almost all are for minor editorial nits. Those that have any substance may well be due to my limited familiarity:

Page 9: In 1 sixth paragraph, "This Framework, does not mandate, requirements" should be "This Framework does not mandate requirements".

Page 9: In 1 sixth paragraph, after "US Government agencies" the period is repeated.

Page 14: In 3.1 first paragraph last sentence, "While, the focus of a CKMS" should be "While the focus of a CKMS".

Page 14: In 3.1 second paragraph, the last sentence seems awkward concerning the double use of "selected". Would an acceptable equivalent statement be "Network characteristics such as error extension properties may also help in the selection of cryptographic algorithms and cryptographic modes of operation, by consideration of their error detection/correction properties"?

Page 15: In 3.1 third paragraph end of second sentence, "shared as must as possible" should be "shared as much as possible".

Page 16: In 3.2 fourth paragraph, the keyword "shall" shall be boldface.

Page 16: In 3.2 fifth paragraph, the keyword "shall" shall be boldface.

Page 16: In 3.4 middle of first paragraph, "Growth adversely impacts, communication," should be "Growth adversely impacts communication,".

Page 18: In 4 first paragraph first sentence, "that will using the CKMS" should be "that will be using the CKMS".

Page 18: In 4.1 first paragraph first sentence, "what information is be collected" should be "what information is to be collected".

Page 23: In 6.1 first paragraph last sentence, a three-way inconsistency is introduced. The text at issue is "[SP 800-57-part1] describes twenty different key types that are shown in Figure 4 below". Figure 4 lists 21 types. SP 800-57 part 1 subclause 5.1.1 lists 19 (it combines the three RNG types in a single entry). I'd suggest either the text and figure should both match SP 800-57 part 1 exactly (19 types), or the text should claim "several different key types".

Page 28: In 6.2 paragraph following list item v (lower case letter v, not roman numeral v), "specify, all bound metadata" should be "specify all bound metadata".

Page 29: In 6.2.1 next to last paragraph second sentence, there is a "shall" rule that is not

boldface.

Page 30: In 6.3.1 list item g, an example is given that "a compromised private signature key might be used ... to verify a signature ...". Shouldn't this say "the public signature key associated with a compromised private signature key might be used ... to verify a signature ..."?

Page 32: In 6.3.2 Transition 10, the transition from suspended to deactivated is described as occurring when the key "is no longer to be used to process data". But the deacivated state is described as allowing processing. Shouldn't the transition be described as occurring when the key "is no longer to be used to protect data"?

Page 36: In 6.4.6 third paragraph, 6.4.6 fourth paragraph, and 6.4.7 second paragraph the combination of multiple independent rules in a single paragraph is inconsistent with practice earlier in the document, where each paragraph contains no more than one rule, or in only four instances, a second rule constraining the means of compliance with the first.

Page 36: In 6.4.7 first paragraph last sentence, the effect of renewal is awkwardly (and self-referentially) stated as "Renewal permits an existing subject key to be renewed beyond its validity period". Would an acceptable alternate statement be "Renewal establishes a new validity period for an existing subject key beyond its previous validity period"?

Page 37: In 6.4.9 first paragraph, several means of key destruction are described, most more complex than overwriting with a zero value. In 6.4.9 second paragraph and three other places in the document, though, destruction is equated to "zeroize", which seems to weaken the requirement. I'd recommend changing the glossary descriptions of Destroyed State and Destroyed Compromised State from "A key lifecycle state that zeroizes a key so that it cannot be recovered and it cannot be used" to "A key lifecycle state in which the key value cannot be recovered and cannot be used". Then remove "zeroize" from footnote 5 on page 26 and remove "(i.e., zeroized)" from 6.4.9 second paragraph on page 37.

Page 37: In 6.4.11 first paragraph third sentence, the example seems inconsistent about the identifier of interest. Change "modify the key identifier without detection" to "modify the key owner identifier without detection".

Page 38: In 6.4.14 first paragraph, the period following the first sentence is duplicated.

Page 38: In 6.4.16 paragraph 1, the migration of archived keying material from old storage media to new storage media is introduced (I can't find such a discussion of archive migration in 800-57) without a necessary warning. Migration of an archival copy to a new medium must include secure erasure of the copy on the old medium; otherwise, the old medium may be inaccessible (read this as "in the hands of an adversary") when the time comes to destroy the key. Simply keeping the archive encrypted is not sufficient, as the archive key may later become compromised. In 6.4.16 paragraph 1 last sentence, change " should be automatically retrieved from the old storage medium and restored on

the new storage medium" to "should be automatically retrieved from the old storage medium, restored on the new storage medium, and securely erased from the old storage medium". Consider constructing a "shall" around the need for specifying secure erasure on archive migration, since this can't be presumed as characteristic of general archive facilities.

Page 39: In 6.4.19 third paragraph, a rule is stated for the CMSM. CMSM is not defined in this standard.

Page 40: In 6.4.22 middle of first paragraph, two sentences are not separated by a period. Change "operational purposes A module" to "operational purposes. A module" (you can reuse one of the redundant periods from elsewhere in the document).

Page 41: In 6.4.28 paragraph 1, the discussion following the first sentence presumes that the "claimed owner" of the private key and the "sending party" (or "sender") of the public key are the same. It would not make sense if a third party possessing only the public key were the "sender". Could this be more clearly identified as an exemplary subcase rather than a required behavior?

Page 45: In 6.6.4 list item d, "Kerbero" should be "Kerberos".

Page 46: In 6.7.1 first paragraph fifth sentence, a conjunction is missing. Change "the function name, the key identifier is presented" to "the function name, and the key identifier is presented".

Page 48: In 6.7.2 first paragraph sixth sentence, there is a misplaced comma. Change "may be generated, within and never leave, the module" to "may be generated within, and never leave, the module".

Page 58: In 8.1 paragraph 2, there appears to be a spurious closing square bracket just before the colon that introduces the list.

Page 60: In 8.2.2 list item d), the unexplained acronym "DMBS" appears. Is it possible that "DBMS" (Data Base Management System) was intended?

Page 85: In Appendix C definition of "Destroyed State", "purposed" should be "purposes".

Page 85: In Appendix C definition of "Destroyed Compromised State", "purposed" should be "purposes".

Page 86: In Appendix C definition of "Key Lifecycle State", "Deactivated Revoked;" should be "Deactivated; Revoked;".

Page 87: In Appendix C definition of "Malware", "includes, spyware" should be "includes spyware".

On 8/2/10 3:32 AM, "Clover, Ian" <Ian.Clover@thales-esecurity.com> wrote:

Comments on NIST SP800-130 Second Draft (June 2010) from Thales e-Security

This is a good holistic document that identifies the areas for consideration when designing a KMS. We've divided our comment into two areas:

- Technical and Content
- Editorial (minor updates covering trivial inconsistencies and typographic errors)

Please contact ian.clover@thales-esecurity.com for further correspondence regarding this document.

The following comments cover Technical and Content observations

No.	Type	Section	Comment
1.	Technical	6	Has any consideration been given to the need for identifying an assured time source to the support key lifecycle?
2.	Content	6.8.3	The requirement for a "separate secure platform" is prescriptive. Built-in protections e.g. fail secure may be perfectly adequate in many systems – particularly in a layered system of protections where built-in protections are running continuously, and are backed up by routine inspections e.g. performed with the system off-line. The specification should allow for flexibility in the design.
3.	Content	8.2.1	Consideration should be given to identifying requirements for hardening and patching of operating system.
4.	Content	12.5 b) and c)	The statements regarding Quantum Computing and Quantum Cryptography may appear inconsistent relatively quickly as implementation advances. Perhaps this section should be reworded to cover new technology in general with "Quantum" technologies being listed less prominently as examples.
5.	Content	12.5 – c)	Current assurance requirements in this field are still in their infancy. Therefore we suggest a downgrade of "shall" to "should".

The following comments cover editorial observations.

No.	Type	Section	Comment
6.	Editorial	3.1 1st paragraph page 15	…key management functions may be shared as must as possible." "Must" should be "much".
7.	Editorial	3.2	There are a couple of instances in this section where 'shall' is not in bold

8.	Editorial	6.1	…[SP 800-57-part1] describes twenty different key types that are shown in Figure 4 below. Fig 4 lists twenty one key types
9.	Editorial	6.2. d)	The Internet Engineering Task Force (IETF) has defined an object identifier for storing various forms of public keys such as DSA, DH, RSA, EC, RSAPSS RSAOAEP, etc It would be useful to include a reference here.
10.	Editorial	6.2 o)	Key Access Control List (ACL): The access control list identifies the entities that can access and/or use the keys as constrained by the "access modes". This framework does not specify the access control list structure. It would be useful to include a reference here.
No.	**Type**	**Section**	**Comment**
11.	Editorial	6.2	A repeated numbering scheme is used in this section. Would it be possible to clarify?
12.	Editorial	6.4.24 6.4.25 6.4.30	6.4.24 and 6.4.25 and 6.4.30 are related in providing an overall trust mechanism. It would be helpful if the sections reference each other to bring out the relationship.
13.	Editorial	6.5 Last two paragraphs on page 43 and first one on page 44	These paragraphs talk about recovery and elsewhere in the document recovery is frequently mentioned. However sections 6.4.17 and 19 make a distinction between recovery and retrieval. It would be helpful if consistent terminology was used throughout the draft.
14.	Editorial	6.8.6	It would be useful reference Section 6.8.5 as the areas are related.
15.	Editorial	6.8.6	There are two sets of items numbered a to c in this section, and item d) has a hanging "…, or".
16.	Editorial	Appendix A, No 10	RFC 3852 is obsoleted by RFC 5652

On 8/11/10 3:04 PM, "Saikat Saha" <ssaha@vormetric.com> wrote:

Hi,

This is a great publication in describing a framework for designing a Cryptographic Key Management Systems. Here are some comments. Some of the comments are minor editorial comments.

1. Section 2.2 Framework Components and Requirements. I have three comments on this.
    - List of example components includes goals and policy. In my understanding Goals and Policy of a CKMS should not be categorized as components along with Key types and key metadata. These should be treated separately.
    - Key Types, Key Metadata and Key Management Functions – From a pure Key Management system design perspective, these three components are inseparable. Primary function of a KMS is to manage and secure keys and all of these components are tied together to perform this primary function. I am not sure I understand how a CKMS can pick one component and not the other.
    - Also, as a guideline, NIST should define a minimum set of components required for a CKMS.
2. Section 3.2 "A CKMS design shall" - "shall" should be highlighted in both sentences.
3. Section 4 "that will using the CKMS" should be "that will be using the CKMS".
4. Section 5 Roles and Responsibility. Can some of these roles be combined? For example, can Key Owner and Cryptographic Officer roles be combined?

   It would be great if Roles (5.1 – 5.7) are part of a sub-section. For example, 5.8, 5.9, 5.10 Separation of Roles and Individuals or 5.11 Requirements involving Roles are not roles.
5. Section 6.1 Key Types "describes twenty different key types"; table below actually shows 21 key types.
6. Section 6.2 Key Metadata. Key Life Cycle State describes 7 states; NIST 800-57 describes 6 key states and does not contain "Revoked". Is "Revoked" a new key state?
7. Section 6.2 m) Security Policies Applicable to the Key. Which policy takes precedence global Security Policy defined as part of Policy component or this local policy? Can they co-exist in a CKMS?
8. Section 6.2 p) version number What is considered as a part of key has been changed? Does it mean bit of the key has been changed which actually means a new key or just some metadata of the key have been changed? Can someone actually change the bits of the same key, is this allowed?
9. e) Method of Distribution, if manual distribution is supported, how will the security of key assured? I do see a value of manual distribution for legacy integration.
10. 6.3.1 Key States Same comment as 6. NIST 800-57 from NIST website mentions 6 key states and does not include "Revoked" state.

On 8/11/10 3:45 PM, "Eddy, Steven [USA]" <eddy_steven@bah.com> wrote:

NISAT,

Attached are my comments on the NIST Draft Special Publication 800-130, dated June 15, 2010, titled "A Framework for Designing Cryptographic Key Management Systems". Unfortunately I will not be able to attend the upcoming conference.

So you know my background, I spent 10 years in the Coast Guard as a pilot. As collateral duties I was the Communications Officer in Puerto Rico for two years, and a CMS Custodian or Alternate for 5. I upgraded the COMSTA from SECTRED to TS. I worked for SAIC for 8 years on the software development team as a training developer, Sr. Systems Engineer, and Test Manager on Tier 1, 2 and 3 of the EKMS System. Worked as Technical Lead IFF Mode 4/5 Crypto Modernization Team, and was Project Manager on developing the Tier 2 to 3 interface for the three IFF Mode 5 equipment types with the Simple Key Loader (SKL). Spent two years working for PEO C4I PMW-160 EKMS/KMI Program Manager, and helped design and architect key loading systems across the Navy and for joint programs. Currently I work as a Systems Security Architect/Engineer for SPAWAR System Center –Pacific on the KMI system.

NIST Comments SP800-130 CKMS, June 15, 2010 Draft

General – Recommend you add an acronym list and sections on training requirements, personal identification requirements, and certificate policy [such as RFC 3647].

Globally – change "key-encryption-key" to "key encryption key" and include in acronyms table as KEK. This is how it appears in the NSTISS 4009 glossary.

Title Page – recommend SYSTEM SECURITY on the waistband rather than COMPUTER SECURITY.

Section 2.1, page 11 – Delete or reword; " (often measured in bits of security)". This is not clear, is it key length or some other parameter. (see comment of pg. 12)

Rephrase "…to bypass by a would-be attacker." to "…for a would-be attacker to bypass."

Section 2.1, page 12 – explain "…security strength (measured in bits of security)".

Section 3.1, page 14 – explain "…error extension properties".

Section 3.3, page 16, last paragraph:

Replace "…workload demands beyond peak workload." with "…increases in peak workloads."

Replace "This specification shall be in terms of additional …" with "This shall be expressed as the relationship of additional …".

Section 4, page 18, first sentence: insert "be" before using.

Section 5.10 - 11, page 22 – Recommend adding a sentence on rotation of duties and mandatory vacation. This can help prevent long term abuses or security threats. Add additional requirement for rotation of duties.

Section 6.1, page 23 – Spell out Random Number Generator (RNG) on first use.

Section 6.4.30, page 42 – Add a reference to IETF drafts on TA Format, TAM Requirements and TAMP. Include these in Appendix A.

Section 6.5, page 43, after

Footnote 11, the link to Wikipedia in Section 7, bottom of page 55 for interoperability takes you to Wikipedia, but states there is no article with that name. Correct link or remove footnote. There is an article in Wikipedia on Interoperability (http://en.wikipedia.org/wiki/Interoperate), of course the problem of imbedding a private link in a document is that the link might change or go away.

Appendix C – Glossary:

Destroyed Compromised State – Remove "or" from "…lifecycle state or that zeroizes…"

Key Label – The two references – "Root CA Private Key 2009-29" and "Maintenance Secret Key 2005" could not be found on the NIST site or when Googled.

Meta-Language – the definition should be expanded to made it clear.

Add: GOTS, Tempest and Tamper to the glossary.

On 8/16/10 2:39 PM, "Benjamin Gittins" <cto@pqs.io> wrote:

Feedback to DRAFT NIST Special Publication 800-130: A Framework for Designing Cryptographic Key Management Systems

Dear NIST,

Thank you for making the opportunity to review and comment on your draft publication.

Please find attached (**as URL**) Synaptic Laboratories Limited's 157 page comment on your excellent draft publication.

http://media.synaptic-labs.com/downloads/pub/publications/NIST/20100816-SLL-NIST-SP800-130-Feedback.zip

The above link contains the comments encoded as a PDF and the original Apple Pages document compressed using ZIP format (16.2 megabytes)

On 8/17/10 11:20 PM, "Vijay Bharadwaj" <Vijay.Bharadwaj@microsoft.com> wrote:

The SP800-130 draft appears to be a very wide-ranging and comprehensive collection of ideas on building and operating secure systems. However, its mission does not appear to be well defined. In particular, from reading Section 5, the document appears to be directed at the designer and operator of the CKMS (e.g. a government agency deploying a CKMS) but the rest of the document mixes requirements that are in such a person's control (e.g. physical security, human processes, warm and cold backups) with others that appear to be at an inappropriate level of detail for such a person (e.g. knowing details of key generation methods, understanding how to incorporate hypothetical future advances such as large-word-size quantum cryptography). Furthermore, some of the requirements (such as Section 11.1.2's architecture review by a panel of internationally renowned experts) appear to be unrealistic for all but the largest and best-funded organizations.

The draft publication lists a total of 179 documentation requirements. It is not clear who would write this documentation, and when, or who would review this document or make decisions based on it. Would a government agency have to write this document before it started deploying a CKMS? Would the document be written in order to formalize the organization's existing processes? Who would compare compliant CKM Systems as suggested in Section 1, and when? More generally, a CKMS is but a small part of an IT organization's infrastructure, and it seems reasonable that organizations would like to integrate it into their overall IT operations. However, this document appears to make such future evolution of IT infrastructures harder, and as a result may impose higher costs on organizations.

We think it would be helpful if the draft was redesigned to be composable with other NIST standards such as FIPS 140. For instance, a CKMS designer using a cryptographic module in a FIPS mode for key generation should not need to document the precise random number generation used, as that should be part of the FIPS 140 validation. This sort of layered approach would also avoid some of the problems mentioned above, by allowing those deploying a CKMS to focus on aspects within their areas of responsibility and expertise. It would also reduce or eliminate redundancies between this document and other standards such as FIPS 140.

On 8/18/10 1:46 PM, "Tsai, Chii-Ren" <chiiren.tsai@citi.com> wrote:

This draft is quite comprehensive. Here are some quick comments for consideration:

1. [Section 3.1] CKMS may not need to cover the generation and storage of ephemeral keys as they are specific to the implementation of each security protocol and seem to be invisible/transparent from key management perspective.
2. [Section 5]
   - Add a new role – Key Custodian. Key custodians are designated to distribute and/or load keys or key components into a target system manually in order to enforce dual control with split knowledge.
   - System Administrators are indeed Information Security Administrators specialized in CKMS. In our environments, system administrators are not involved in IS related administration.
   - Cryptographic Officer may not be a standalone role. It is commonly assumed by Information Security Officer.
   - Suggest not to mention reporting hierarchy as roles could spread in various businesses/organizations within an enterprise and may not have the org chart.
3. [Section 6.2]
   - The Security Strength of the Key may not be necessary as it is dictated by the underlying cryptographic algorithm and key length being used and is also a moving target over time.
   - Parent Key may not be needed. If keys are derived from a parent key with a mathematical function, presumably the child keys may not need to be managed by the CKMS as they would be generated automatically on demand.
   - Key Access Control List (ACL) may include exportable. If a key is exportable, it means the key can be exported to be installed on another system. Therefore, the CKMS must support a function to export the key by encrypting the key with a transport key for distribution and such process may be enforced with dual control or multiparty control.
4. [Section 6.3.1]Compromised state may not be necessary. Once a key is compromised, a manual process would kick in to revoke or deactivate the key. For example, if a signature key is compromised, the private signature key is revoked immediately and the public signature key may be retained or deactivated to verify previous signatures in archive. As a result, the revocation reason of the key's meta-data would be "compromise."
5. [Section 6.4.16] Key archive must comply with data retention policy. If encrypted data along with associated cryptographic keys must be retained for the same period of time.
6. [Section 6.7.1] All administrative access to the CKMS must be logged/audited for accountability.

7. A CKMS may be used to centrally manage cryptographic keys in various systems within an enterprise. It may be constructive to highlight a reference architecture of such a CKMS with the Key Management Interoperability Protocol (KMIP).